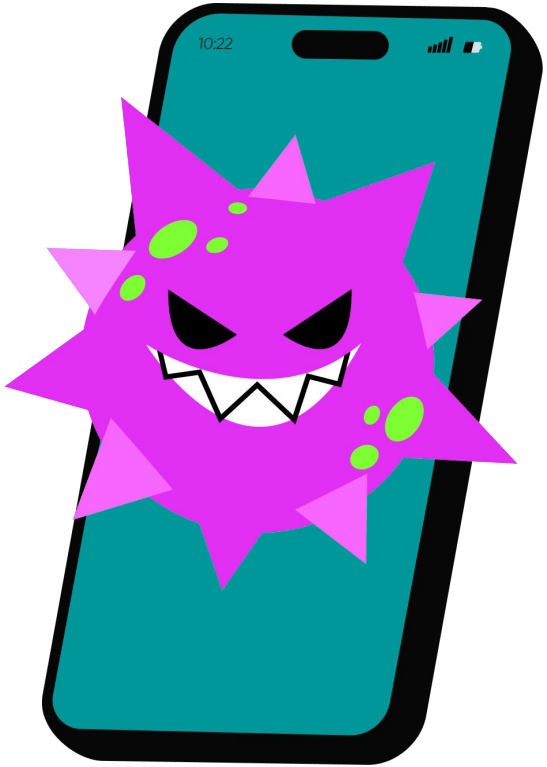
Сезон 2022/2023

Что прячется в смартфоне: исследуем мобильные угрозы

УРОК ЦИФРЫ kaspersky

Какие существуют примеры вредоносных приложений?

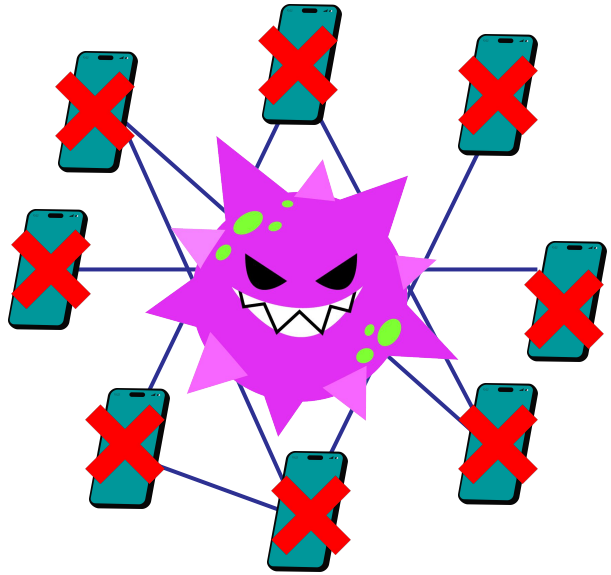


Какие существуют примеры вредоносных приложений?

Для мобильных устройств актуальны почти все те же угрозы, что и для ПК, в том числе вредоносные программы. Примеры таких программ:

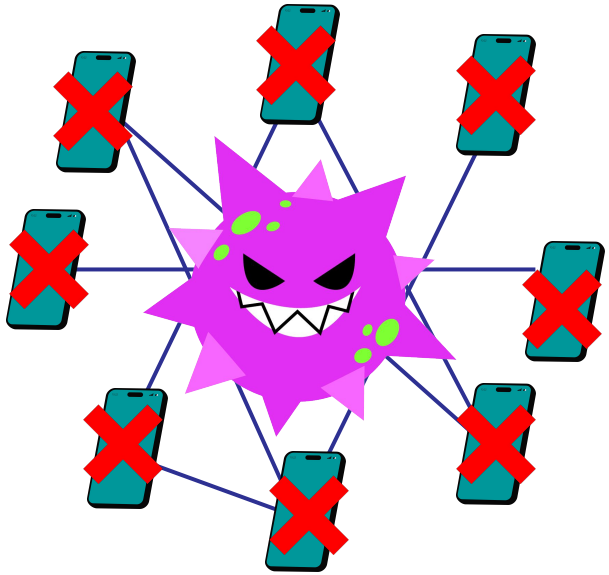
– Троянцы
– Программы-вымогатели
– Скамерские приложения

Что делать, если устройство оказалось заражено вредоносной программой?



Что делать, если устройство оказалось заражено вредоносной программой?

Мы не рекомендуем пытаться избавиться от вредоносных программ самостоятельно: для этого детям следует обратиться за помощью к взрослым и использовать защитные решения.



Сегодня на уроке

- Познакомимся с понятиями «фишинг» и «скам»
- Узнаем, какие специалисты помогают сделать нашу цифровую жизнь безопаснее
- Узнаем, как защититься от киберугроз и противостоять уловкам злоумышленников

Что означает понятие «мобильные угрозы»?

Что означает понятие «мобильные угрозы»?

Это различные киберугрозы, направленные на пользователей мобильных устройств.

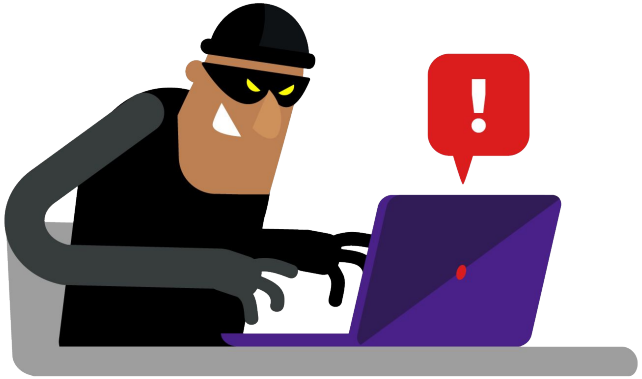
Сталкивались ли вы с мобильными угрозами?

Может быть слышали в новостях? Или кто-то из ваших знакомых сталкивался со злоумышленниками? Сталкивались ли вы с заражением вашего смартфона? Или с попыткой украсть ваш аккаунт в мессенджере?

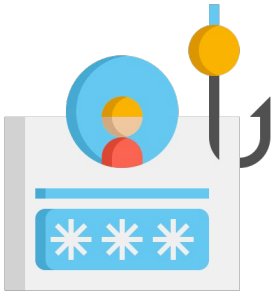
Для чего злоумышленники атакуют мобильные устройства?

Для чего злоумышленники атакуют мобильные устройства?

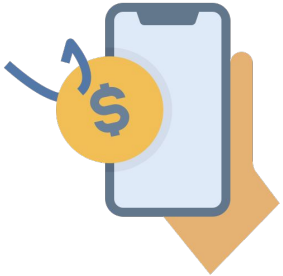
Злоумышленники преследуют выгоду! Например, хотят получить деньги, доступ к ценной информации, или же пытаются намеренно причинить вред организациям или отдельным людям.



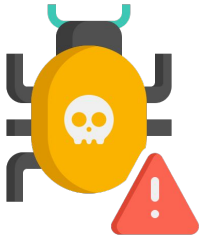
Примеры угроз, с которыми могут столкнуться пользователи смартфонов



Фишинг



Скам



Вредоносное ПО

Фишинг

Фишинг – процесс выманивания конфиденциальной информации у пользователя (логин и пароль, данные банковской карты). Например, злоумышленники могут пытаться украсть аккаунт в мессенджере или социальной сети с помощью поддельных ресурсов, где побуждают ввести данные для входа в учетную запись.

Примеры скама

Скам — вид онлайн-мошенничества, при котором пользователю предлагают щедрое денежное вознаграждение. С такой угрозой пользователи могут столкнуться в интернете в виде скам-сайтов и в виде приложений. После скачивания такого приложения пользователя перенаправляют на страницу ввода личных данных. Затем на экране отображается размер якобы положенной человеку компенсации или выигрыша. Далее пользователя просят заплатить «комиссию», например, за вывод средств. Если человек это сделает, то злоумышленники получат свою прибыль — в виде этой «комиссии», а пользователь только потеряет деньги, не получив ничего взамен

Примеры вредоносного ПО

Троянцы – это вредоносные программы, осуществляющие несанкционированные пользователем действия: они уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей.

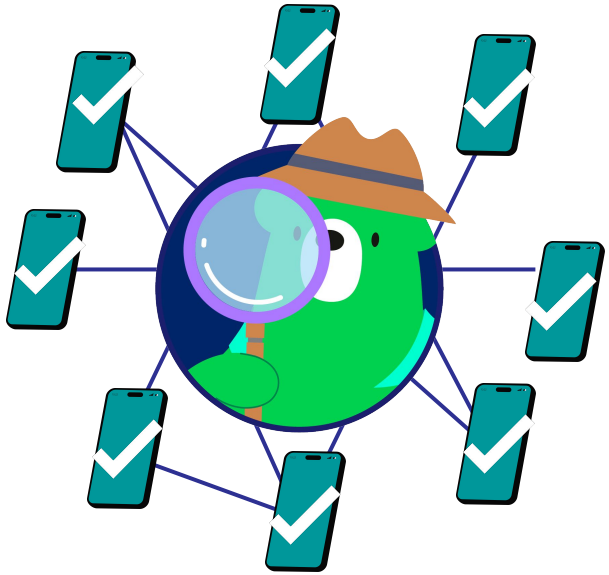
Программы-вымогатели – это вредоносное ПО, которое шифрует данные или блокирует доступ к ним и требует заплатить выкуп за снятие блокировки или дешифровку файлов.

Какие специалисты помогают улучшать технологии защитных решений?

- Эксперты по кибербезопасности
- Разработчики защитных решений для мобильных устройств
- Контент-аналитики
- Спам-аналитики

Какие специалисты помогают улучшать технологии защитных решений для мобильных устройств?

Эксперты по кибербезопасности изучают и анализируют мобильные угрозы, разработчики и тестировщики отвечают за создание защитных решений. Контент-аналитики помогают совершенствовать технологии, которые распознают фишинговые или скам-ресурсы. Спам-аналитики изучают методы и схемы спам-рассылок.



Какие действия помогут защититься от злоумышленников?

- Прежде чем что-то скачать в интернете или принять участие в крайне щедрой акции, **обязательно перепроверяйте информацию в официальных источниках**.
- **Скачивайте приложения только из официальных источников** (официальные магазины приложений или сайты компаний). Такие приложения (и их обновления) проходят модерацию на наличие вредоносного кода.
- **Запретите установку приложений из неизвестных источников.** Исключение можно сделать только для официальных магазинов приложений и официальных сайтов компаний.
- **Регулярно обновляйте программы и операционную систему.** Вместе с обновлениями разработчики исправляют ошибки и уязвимости в ПО.

Какие действия помогут защититься от злоумышленников?

- **Установите антивирус и регулярно его обновляйте.** Решение защитит ваши данные и устройство от различных вредоносных и нежелательных программ, не даст перейти по фишинговой ссылке.
- **Используйте надежные пароли**, **которые трудно подобрать и не храните их в открытом доступе**.
- **Используйте двухфакторную аутентификацию** — это способ защитить свой аккаунт, даже в том случае, если логин и пароль от него знают злоумышленники. Обычно это выглядит так: первый шаг — это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или на электронную почту. Варианты могут быть разными.

Какие действия помогут защититься от злоумышленников?

- **Не переходите по ссылкам из подозрительных сообщений в почте, мессенджерах и социальных сетях.** За такими ссылками может скрываться фишинговый или скам-ресурс.
- **Не сообщайте конфиденциальную информацию незнакомым людям.** Злоумышленники могут маскироваться под знакомых, дальних родственников или сотрудников банка, писать в социальных сетях или даже позвонить.
- **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос.** Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте и убедитесь, что вам звонили не злоумышленники.

Какие действия помогут защититься от злоумышленников?

- **Внимательно проверяйте адреса веб-сайтов прежде, чем вводить на них конфиденциальную информацию.** Обращайте внимание на URL-адреса сайтов, совпадают ли они с настоящими.
- **Когда устанавливаете приложения на смартфон, не давайте им доступ к тем разрешениям и функциям, которые им не нужны для корректной работы.**
- **Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.** Помните, что только лишь закрыть вкладку недостаточно, нужно нажать кнопку «выход» из своей учетной записи в социальной сети, мессенджере или любом другом сервисе.

Отдельно остановимся на паролях

Пароль — это одна из важнейших составляющих безопасности аккаунтов. Здесь нужно придерживаться следующих правил:

- пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы;
- меняйте пароли регулярно и используйте уникальные пароли для разных сайтов;
- если у вас есть подозрение, что ваш пароль и логин оказались у злоумышленников или в открытом доступе, как можно скорее поменяйте пароль;
- в пароле не должно быть личной информации, например, имени питомца или номера телефона;
- двухфакторная аутентификация поможет быстро восстановить доступ к аккаунту и сменить пароль;
- не храните пароли на листочках и в текстовых файлах на компьютере. Для этого лучше использовать специальные программы — менеджеры паролей.

Давайте вместе проверим, насколько хорошо вы знаете правила информационной безопасности

Приготовьте лист бумаги и ручку.
Напишите числа от 1 до 10.

Вопрос 1: Посмотрите на адрес (ссылку) https://shkola.ru. Что означает S в HTTPS?

A. S = secure, потому что соединение зашифровано

B. S = simple, упрощенный и более быстрый протокол

C. S = school, значит сайт образовательный

D. Множественное число

Вопрос 2: Что такое фишинговый сайт?

A. Мошеннический сайт, маскирующийся под настоящий

B. Сайт с афишами

C. Сайт, защищенный шифрованием

D. Сайт про рыбалку

Вопрос 3: Как распознать фишинговый сайт?

A. Изменился дизайн сайта (цвет, логотип и т.д.)

B. Изменилось доменное имя, хоть и осталось похожим на оригинал

C. На странице просят оперативно ввести логин и пароль или перевести деньги

D. Все вышеперечисленное

Вопрос 4: Какой пароль безопаснее?

A. QWERTY123

B. qazwsxedc

C. y@uD65fk31

D. vasya1985

Вопрос 5: Вам предлагают принять участие в тестировании продолжения популярной игры, скачав файл с неофициального сайта. Ваши действия?

A. Соглашусь, только в том случае, если давно играю в эту игру и хорошо знаю правила

B. Если это эксклюзивное предложение, то соглашусь

C. Не буду реагировать на такие предложения

D. Посоветую друзьям

Вопрос 6: Приложение просит доступ к SMS и осуществление звонков, я…

A. Все предоставлю как просит приложение

B. Откажусь и не буду пользоваться приложением никогда

C. Соглашусь, если эти права нужны для работы приложения

D. Всегда запрещаю все

Вопрос 7: Как чаще всего действуют онлайн-мошенники?

A. Подбрасывают пользователям оптические диски (CD, DVD)

B. Незаметно втыкают флешки в компьютеры жертв.

C. Раздают флаеры на улице

D. Используют социальные сети, мессенджеры, электронную почту и рассылают там фишинговые или скам-сообщения

Вопрос 8: Вас просят по телефону сообщить номер вашей банковской карты, ваши действия?

A. Конечно сообщу, собеседник представился сотрудником банка в котором у меня карта

B. Не буду сообщать, сам перезвоню в банк

C. Сообщу только если он назовет мои ФИО и историю операций по карте

D. Скажу только логин и пароль от онлайн-банка, пусть разбираются

Вопрос 9: Что такое овершеринг?

A. Сервис по аренде автомобилей через смартфон

B. Чрезмерная публикация информации о себе в интернете

C. Флешмоб на YouTube, в котором люди делятся с друзьями видео

D. Перенаселенная коммунальная квартира или общежитие

Вопрос 10: Как эффективнее защититься от мошеннических и спам-звонков?

A. Не отвечать на звонки с незнакомых номеров

B. Установить специальную программу, которая будет определять такие звонки

C. Регулярно обновлять операционную систему и приложения

D. Нигде не оставлять свой номер телефона

Вопрос 11: Какой мобильный браузер самый безопасный?

A. В котором есть удобная поисковая система

B. Тот, у которого удобный/красивый дизайн

C. Любой браузер будет безопасным

D. Браузер самой последней версии

Вопрос 12: Что такое спам в мессенджере?

A. Тип вируса

B. Ложная статья на новостном сайте

C. Нежелательное сообщение

D. Негативный комментарий

Проверим ответы

№	Ответ:
1.	A
2.	A
3.	D
4.	C
5.	C
6.	C
7.	D
8.	B
9.	B
10.	B
11.	D
12.	C

Ответили верно, ставьте «+»,

если нет, то «–».

Подсчитайте количество «+».

Результаты викторины

11–12 баллов. Поздравляем, вы надежно защищены!

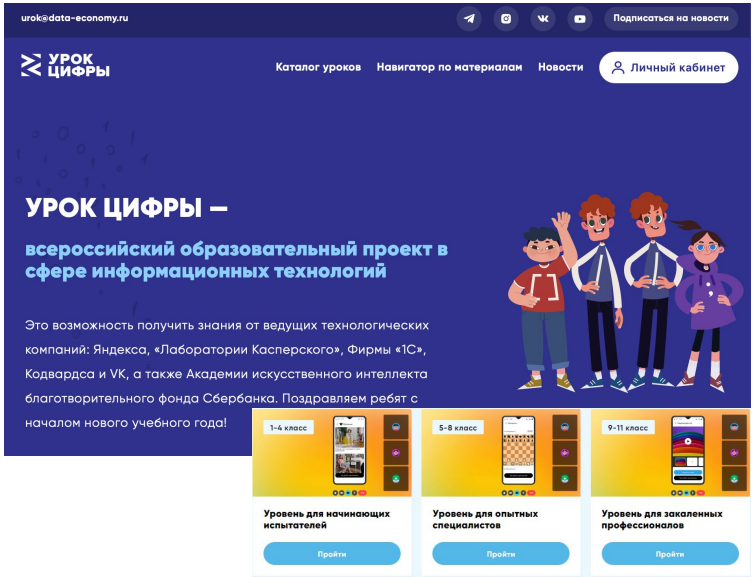
9–10 баллов. Хороший результат, но есть над чем поработать.

0–8 баллов. Нужно изучить правила информационной безопасности.

Домашняя работа

Зайдите на сайт [урокцифры.рф](), найдите урок «**Что прячется в смартфоне: исследуем мобильные угрозы**», выберите тренажер для своего возраста.

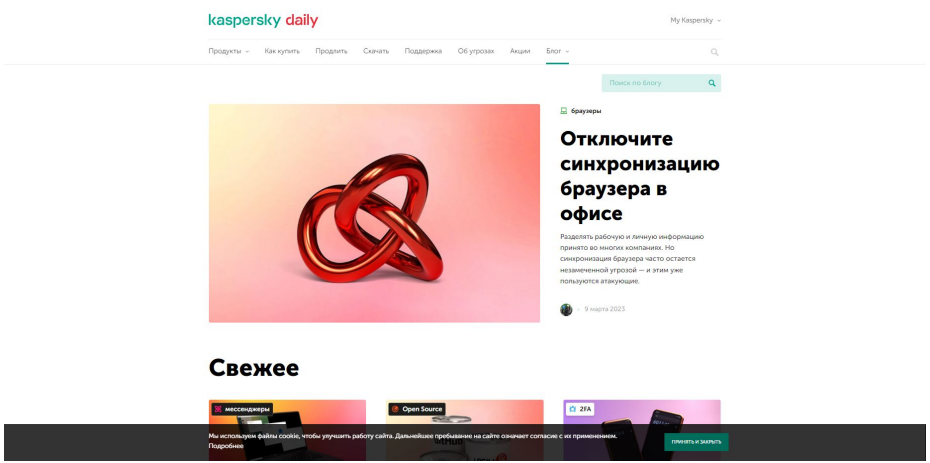
Пройдите тренажер для своего класса и получите сертификат о прохождении урока.



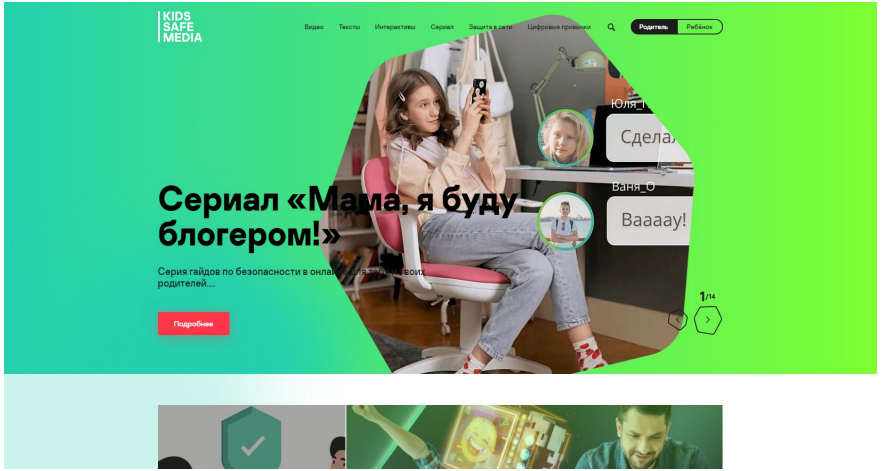
Подведем итоги

- Что больше всего запомнилось из урока?
- Что нового и полезного узнали?
- Что будете использовать в повседневной жизни?

Полезные ресурсы



www.kaspersky.ru/blog/



kids.kaspersky.ru